

IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
FLORENCE DIVISION

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING A
SEARCH WARRANT FOR A HEWLETT
PACKARD LAPTOP COMPUTER, SERIAL
NUMBER 5CD9518R17

MISC. NO.: 4:22 cr 855-TER

AFFIDAVIT

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT
AND SEIZURE WARRANTS**

I, Eric G. Elliott, Special Agent, United States Department of Justice, Drug Enforcement Administration ("DEA"), being duly sworn, hereby state as follows:

Introduction

1. I respectfully submit this affidavit in support of an application for a warrant to search the following:

- a. Hewlett Packard Laptop Computer, Serial Number 5CD9518R17, which is currently held as evidence at the Horry County Police Department, 2560 N. Main Street, Conway South Carolina, 29526 (hereinafter **SUBJECT COMPUTER**)

SUBJECT COMPUTER is a device believed to be owned and utilized by TRAVIS M. SPIVEY. SPIVEY owns and operates TASTE OF EXOTICS LLC, a purported "candy store" located at 3926 Wesley Street, Building 500, Unit 503, Myrtle Beach, South Carolina. Agents have determined SPIVEY utilizes the business as a "front" or cover for the sale of suspected marijuana and marijuana edibles.

This affidavit will show a pattern of criminal behavior as well as establish probable cause that **SUBJECT COMPUTER** contains evidence of criminal activity perpetrated by SPIVEY and his co-conspirators.

Agent Background

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 21 United States Code Section 878; an Affiant empowered by law to conduct investigations of, and to make arrests for offenses enumerated in Title 21 of the United States Code. Since September 1997, I have been employed as a Special Agent with the DEA. I have received specialized training in narcotics investigation and identification, as well as the laws of criminal conspiracy, search and seizure and associated financial crimes, including money laundering.

During the course of my law enforcement career, I received training in the utilization, preparation, and execution of search and seizure warrants. I have received additional training in the investigation of financial crimes, specifically the laundering of proceeds derived from the sale of illegal narcotics. I have subsequently executed numerous search and seizure warrants for narcotics, dangerous drugs, as well as documents, records, books, and proceeds derived as a result of this illicit activity. I have been the case agent or co-case agent for several cases involving high priority targets and multi-agency investigations under the Department of Justice's Organized Crime Drug Enforcement Task Force (OCDETF) program, which targeted major drug trafficking/money laundering organizations and the related criminal activity. Furthermore, I have arrested numerous individuals for violations of State and Federal narcotics statutes.

3. During my employment, I have been tasked with various narcotics and related criminal investigations including firearm offenses and money laundering. Based on these investigations, I have gained experience with the use of a variety of law enforcement techniques to include the following: analysis of financial, business, and personal records in both written paper and digital format; witness interviews; controlled narcotics purchases; utilization and handling of Confidential Informants; Mutual Legal Assistance Treaties; Ex Parte applications for tax information; utilization of electronic and wire interceptions; the utilization of cooperating witnesses and consensual recordings; the use of physical surveillance techniques including the use of pole cameras and recorders; the use of geographic analysis information regarding mobile telephone systems; the analysis of historical telephone records and the utilization of pen register and trap/trace devices; the analysis and review of computers to include desktops, laptops, tablets and PDA devices; the analysis and review of computers and digital media storage devices; cell phones and smart phones to include stored data, texts and call logs; and various other types of electronic surveillance techniques such as body wires and transmitters. Additionally, I have provided testimony under oath in various judicial proceedings on numerous occasions in multiple Federal Judicial Districts as well as various state courts. The matter for which testimony was given in court proceedings was related to criminal investigations conducted as a DEA Special Agent as well as expert testimony. Affiant has participated in and conducted money laundering investigations where the source of funds was determined to be proceeds of illicit narcotics sales. Affiant has specifically investigated and participated in the indictment and prosecution of individuals who have utilized business fronts as a method to integrate illicit profits in order to conceal the true source from where derived. The actions and methods of operation found in previous narcotics and financial investigations mirror the steps and systematic approaches taken by the target(s) of this current investigation which have been identified thus far and are delineated in the paragraphs below.

4. I have investigated domestic and international criminal drug organizations that operate over a wide geographic area and receive US Currency as payment in return for the narcotics they distribute. I have investigated and traced this associated currency, which is returned to suppliers for purchases made with profits invested and/or laundered through various techniques to conceal the source of their illicit activities (including the use of front companies, straw buyers, and nominee-named owners). I have been the affiant on numerous search, seizure, and arrest warrants, including but not limited to warrants for telephones, smart phones, residences, businesses, bank accounts, and safety deposit boxes.

5. The facts set forth in this Affidavit are based on my personal participation in the investigation described herein and upon information from the following sources, which I believe to be reliable:

- a. Oral and written reports, records, interviews, debriefings, and other evidence regarding this investigation from Special Agents, as well as other state and local law enforcement officers;
- b. Surveillance and enforcement activities;
- c. Review of digital media, documents, photographs, and other evidentiary items gathered during this investigation.

6. Because this Affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not included each and every fact known to me concerning this investigation. Rather, I have set forth only those facts that I believe are sufficient to establish the necessary probable cause for the requested search warrant. In addition, where I report information provided by others or from reviewing documents and records, such information is provided in relevant part.

Applicable Statutes

7. As set forth below, there is probable cause to believe the user of **SUBJECT COMPUTER**, along with his co-conspirators, committed the following violations. There is also probable cause to believe that the items described more fully in Attachment B constitute evidence, contraband, fruits, and instrumentalities of these violations and may be found on **SUBJECT COMPUTER**. Violations include:

- i. 21 U.S.C. § 846 (conspiracy to possess with intent to distribute a controlled substance);
- ii. 21 U.S.C. § 841(a)(1) (possession with intent to distribute a controlled substance);
- iii. 18 U.S.C. § 1956(a)(3)(A), (a)(3)(B), and (h), concealment and/or promotion money laundering, and/or a conspiracy to violate these statutes.

The Underlying Investigation

8. This investigation has targeted a significant Drug Trafficking Organization (DTO) which is involved in the distribution of marijuana and marijuana related items. Throughout this investigation, agents/officers have continued to attempt to identify all individuals involved, their specific roles within the organization and the potential crimes committed. Based on the facts learned thus far, **SUBJECT COMPUTER** was seized from a location where bulk marijuana was stored, illicit distribution activities were occurring and extensive recording keeping of the events were maintained.

SUBJECT COMPUTER

9. **SUBJECT COMPUTER** is a Hewlett Packard Laptop Computer, Serial Number 5CD9518R17, believed to be owned and utilized by SPIVEY.

10. On August 25, 2022, Horry County Police Department patrol officers responded to TASTE OF EXOTICS LLC, 3926 Wesley Street, Building 500, Unit 503, Myrtle Beach, South Carolina for an alarm activation. Officers who arrived at the location discovered a large quantity of a green leafy substance, suspected to be marijuana. The address location is described as a two-story office building. The first floor of the building has a large open area in the front where true candy items are sold. There are two rooms off of the large open area in which approximately 20 pounds of a green leafy substance (suspected marijuana) was found. The second floor of the building has a large main room that is set up like a living room, containing a desk and couch. There are two smaller rooms located off the main room, in which approximately 289 pounds of a green leafy substance (suspected marijuana) was found.

11. A state search warrant was sought and obtained for the property seeking evidence of illegal narcotics, including currency obtained through illegal drug trafficking and/or distribution, documentation and records, including electronic media, of any illegal drug interactions, any items used to conduct or facilitate illegal drug trafficking, any books or ledgers documenting illegal transaction and/or receipts for purchases and/or shipments of illegally possessed drugs, any documents and/or electronic media.

12. During the execution of the state search warrant, the approximately 309 pounds of suspected marijuana was seized along with various other items. A quantity of "vape cartridges" containing suspected Tetrahydrocannabinol (THC), as well as edible "Gummies" with suspected THC was seized. The packages of THC items stated the THC content was 75% to 80%. In the upstairs large main room on top of a desk were a "Doctor's Care" receipt in the name of TRAVIS SPIVEY, a lease agreement for the property naming the tenant as TRAVIS SPIVEY, a spiral notebook, and the **SUBJECT COMPUTER**. In each of the smaller upstairs rooms containing the suspected marijuana, note pads were located which contained handwritten notations recognized to be "drug ledgers" referring to suspected marijuana received and sold. The suspected marijuana was contained in plastic vacuum-sealed bags which affiant recognizes as a common method found in numerous prior investigations. Furthermore, an electric vacuum sealer was located inside the property with the suspected marijuana, indicating larger quantities of bulk marijuana were potentially broken down into smaller quantities and repackaged at the location.

13. A review of the spiral notebook and note pads revealed detailed, handwritten notes, in two distinctly different handwriting styles, including quantities and dollar amounts related to the purchase of marijuana and THC items which were suspected to be sold from the location. Additionally, general business information with names, social security numbers, and addresses of individuals were identified in the notations. Based on affiant's training and experience, the notations were identified as ledgers evidencing various amounts of currency paid and collected for marijuana bought and sold.

14. A review of handwritten ledgers and notations on marker boards on the wall inside the property showed numerous writings recognized by affiant to be names, types or strains of marijuana sold. The notation "What I Paid" was written on a board with an arrow pointing at fourteen lines of names and numbers recognized to be types of marijuana and suspected cost per pound. An example of some of the notations include: "PC-800"; "Kush Cake-1100"; "Purple Punch-1100"; "Oreo Cookie-1000"; and "Gelato-1000."

15. An analysis of a second marker board showed extensive notations, a sample of which include: "8 - Bubba"; "8 - Bob"; "4 - Bob#1"; "14 - Bob 200"; "Bubbas 850 - 3"; and "B1 850's - 17."

16. Another marker board inside the location had additional handwritten notations which affiant recognized to be possible strains or types of marijuana, a sample of which included: "Push-305"; "Simpsons -10"; "Nova - 16"; "Gold Coast - 10"; "Exotic Fiz - 50" and "Cake - 450."

17. Affiant is aware based on the quantity of suspected marijuana, marijuana edibles and THC vape cartridges found, coupled with the extensive notations of such activities in the form of ledgers, significant narcotics distribution activities were being handled or coordinated at the property. As such, extensive currency would be exchanged as payments for both wholesale purchases and resale to customers. Affiant is aware this would generate illicit data necessitating an excessive need for record keeping on the illegal activities.

18. Affiant has on numerous occasions conducted investigations where ledgers, both handwritten and computer generated, were utilized to maintain transactional, profit and expense data as records of drug sales. Due to the apparent large-scale operation which included a variety of customers and strains or types of suspected marijuana with various prices, thorough and comprehensive records were necessary for the operation and may also be contained on **SUBJECT COMPUTER** which was found contemporaneous to the other evidence.

19. Affiant conducted an inquiry of law enforcement indices and databases which revealed SPIVEY was previously arrested in 2011 for firearms and again in 2015 for narcotics offenses. Furthermore, law enforcement interviews of a cooperating witness in 2017 identified Spivey as being involved in the distribution of narcotics.

Summary of Probable Cause and Basis for Items to be Seized

20. Based on the foregoing, I respectfully submit that there is probable cause to believe that the **SUBJECT COMPUTER** presently contains evidence of crimes under investigation committed by SPIVEY as well as his associates and co-conspirators. Evidence shows SPIVEY utilized **SUBJECT COMPUTER** inside the location and property where significant drug activities occurred which would necessitate the recording of drug sales, profits, and expenses.

21. **SUBJECT COMPUTER** is believed to contain additional evidence, to include, but not limited to: photographs of narcotics; names, addresses, and phone numbers of associates, co-conspirators, suppliers, and any individuals involved in his criminal activities; evidence of drug and money laundering activities, to include correspondence with individuals who assist in the movement or distribution of narcotics or the expenditure of illicit US Currency; and evidence of

money laundering activities, to include correspondence with individuals who assist in the illicit layering and placement of currency into investments to disguise the true source of the funds.

22. Based on my training, experience, participation in this investigation (and others with similar schemes involving narcotics distribution and money laundering), and consultation with other experienced law enforcement officers, I offer the following basis to seize the items listed in Attachment B as evidence, fruits, and instrumentalities of the crimes under investigation:

- a. Individuals engaged in narcotics distribution and money laundering regularly conceal fruits of their illicit activities, to include large amounts of currency, financial instruments, precious metals, jewelry, and other items of value and/or proceeds of illegal activities, and evidence of financial transactions relating to obtaining, transferring, secreting, or spending of large sums of money made from engaging in illegal activities in locations that offer security from detection and theft to include residences, businesses, offices, garages, storage buildings, safes, vaults, safety deposit boxes, and/or automobiles;
- b. Narcotics traffickers often purchase and/or title their assets in fictitious names, aliases, names of relatives, criminal associates, or business entities to avoid detection of these assets by government agencies. Even though these assets are in the names of persons other than the drug trafficker, the trafficker usually owns, uses, and maintains dominion and control over these assets.
- c. Narcotics traffickers maintain books, records, receipts, notes, ledgers and other papers relating to the procurement, distribution, storage, and transportation of controlled substances. These documents include but are not limited to: records showing the phone numbers of customers, the amount of controlled substances "fronted" to various customers along with running totals of debts to customers. Drug traffickers frequently maintain receipts such as credit card billings, parking stubs, hotel reservations/records, airline tickets, gas receipts and various notes. Items used to package controlled substances are also frequently maintained by drug traffickers. It is also common for these traffickers to maintain electronic devices that are used to facilitate their criminal activities, to include, but not limited to, computers, electronic tablets, mobile telephones, paging devices, answering machines, police scanners and money counters. In the current transformation of society to a more digital media platform, many of the above-described records and notations are held and maintained in digital storage devices such as phones, computers and digital media storage devices held within.
- d. Individuals engaged in money laundering misrepresent the negotiations for, transactions for, and provision of, sales/services, whether executed, delivered, or proposed or otherwise discussed. Documents that reference corporate purchases, sales, services, whether executed, delivered, or proposed or otherwise discussed, and their corresponding payments/receipts, can be evidentiary by the inclusion, omission, or alteration of known or represented purchases/sales. A partial list of these corporate documents include the following: contracts or agreements; sales journals; purchase journals; cash receipt journals; cash disbursement journals; invoices; sales receipts; purchase orders; receiving reports; inventory records; and shipping record;

- e. Bank records that reflect assets, liabilities, payments, and receipts can be evidentiary for misrepresenting the nature, source, and ownership, of transactions of individuals, corporations and corporate assets; and for misrepresenting the negotiations for, transactions for, and provision of, sales/services; by the inclusion, omission, or alteration of known or represented assets, liabilities, payments, and/or receipts. Multiple types of accounts can be used to hold assets, reflect liabilities, make payments, and receive funds to include checking, savings, money market, NOW, TIME, CDs, security, credit/charge, and retirement accounts. A partial list of these bank records for these types of accounts include the following: bank statements; canceled checks; deposit tickets; copies of items deposited; credit and debit memos; loan applications; loan statements; loan correspondence including letters to/from banks, notes/memoranda to file, collateral agreements and documents, credit reports, notes reflecting obligations to pay, real estate mortgages, and loan amortization statements; confirmation slips; Fed Wire, SWIFT, or other money transfer or message documents; safe deposit contracts and entry records; application for credit; credit card statements; and charge card statements. Therefore, documents that reference corporate and personal assets and/or liabilities can be evidentiary;
- f. It is common today for persons to use multiple methods of communication to conduct business. Individuals involved in illegal activity utilize the same methods of communication to conduct business. Therefore, any and all forms of communication (records, documents, programs, applications, or materials), including those in an electronic format, that contain, reference, or relate to the items listed in preceding paragraphs to include: correspondence, communications in written or electronic form, including but not limited to, letters, faxes, emails, proposals, agreements, contracts, and records, regarding the business entities provided in this application.
- g. It is common today for individuals and small businesses to maintain records electronically on personal computers, telephones, smart phones, personal data tablets and network servers maintained inside of their residences and/or businesses.
- h. Individuals intending to distribute controlled substances often maintain quantities of controlled substances, as well as scales, packaging and cutting materials, inside of their home or distribution locations.
- i. It is common in the purchasing, selling and distribution of controlled substances for drug traffickers to "front" drugs (providing narcotics on consignment) to several clients causing large debts to be incurred. Often times these drugs/debts are paid for in installments over a period of time and involve large amounts of currency to exchange hands. Because of the large amounts of drugs and debts involved, and to prevent discrepancies, it is necessary for records such as, but not limited to, papers, notes, ledgers, journals, and logs to be maintained by these drug traffickers. Frequently, these records are kept and concealed where the traffickers have ready access to them, i.e., homes, offices and automobiles.

- j. Drug traffickers take, or cause to be taken, photographs and/or video of themselves, their associates, their drug proceeds or assets derived from the sale of controlled substances. These traffickers usually maintain these photographs and/or the videos in their possession on personal smart phones, computers and other digital media storage devices as well as at their residences and stash locations.
- k. Drug traffickers must maintain, on hand, amounts of United States currency in order to maintain and finance their ongoing drug business.
- l. Persons engaged in drug trafficking commonly conceal large amounts of currency, financial instruments, precious metals and other items of value. It is common for drug traffickers to purchase items costing over ten thousand dollars. The reporting requirements, commonly referred to as CTR's for transactions over ten thousand dollars, cause tremendous problems for narcotics traffickers when they attempt to negotiate their illegal profits at a financial institution. In doing so, traffickers will often violate federal structuring/Currency Transaction Reporting laws (Title 31, United States Code, Section 5324) by obtaining several cashier's checks/money orders in small increments from several institutions. Often the traffickers utilize "smurfs" to purchase these checks and/or money orders that generate receipts from these checks. The proceeds of drug transactions, and evidence of financial transactions relating to obtaining, transferring, secreting or spending large sums of money obtained through engaging in narcotics activities are maintained by drug traffickers in their residences, businesses, automobiles and at similar locations of their co-conspirators.
- m. Unexplained wealth is probative evidence of crimes motivated by greed, in particular, trafficking in controlled substances. I further recognized that the small and medium denominations of currency, along with the manner in which the currency is handled, carried and concealed, may establish probable cause that there is a substantial connection between the questionable currency and narcotics transactions.
- n. Therefore, there is probable cause to believe evidence of the criminal activity to include: conspiracy to possess with intent to distribute a controlled substance, a violation of 21 U.S.C. § 846, possession with intent to distribute a controlled substance, a violation of 21 U.S.C. § 841(a)(1), and ????? concealment promotion and money laundering conspiracy, a violation of 18 U.S.C. § 1956(a)(3)(A), (a)(3)(B), and (h) will be located on **SUBJECT COMPUTER**.

SEARCH AND SEIZURE OF DIGITAL EVIDENCE

23. This application seeks authorization to search for and seize evidence of the crimes described above in whatever form they are found, including evidence of how the **SUBJECT COMPUTER** was used, the purpose of its use, and who used it.

24. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant.

25. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

26. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

27. *Latent Data:* Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

28. *Contextual Data:* In some instances, the computer writes to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a picture of what the

computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

- a) Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.
- b) Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

29. Based on the foregoing and consistent with Rule 41 (e)(2)(B), in searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

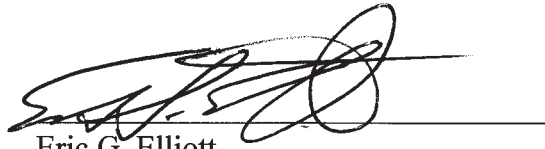
- a) Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.
- b) Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a hash value library to exclude normal operating system files that do not need to be searched. In addition, law

enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

- c) Law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 60 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 60-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 60 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 60-day period from the date of execution of the warrant.
 - d) If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.
 - e) If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.
30. The government will retain a forensic image of the **SUBJECT COMPUTER**.

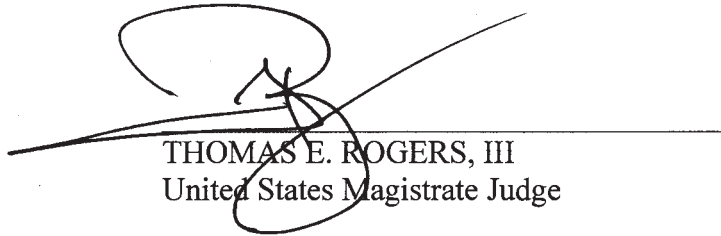
Summary and Request for Sealing

31. Based upon the foregoing, I respectfully request a search warrant be issued for the **SUBJECT COMPUTER**.
32. This affidavit has been reviewed by Assistant United States Attorney Everett McMillian.



Eric G. Elliott
Special Agent
U.S. Drug Enforcement Administration

Subscribed and sworn to before me this 7 day of October, 2022.



THOMAS E. ROGERS, III
United States Magistrate Judge